证　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2003.06.13

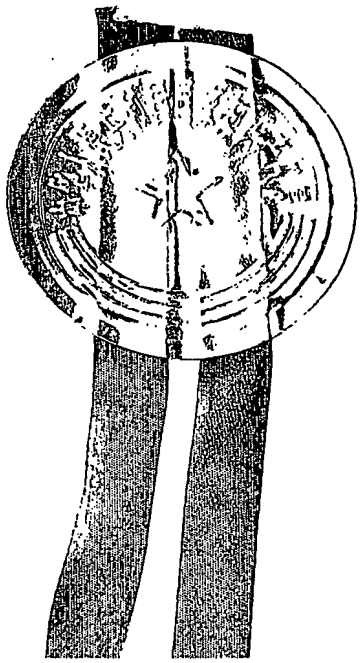
申　请　号：　03137109.4

申请类别：　发明

发明创造名称：　基于U S B 闪存盘存储介质私有空间的验证方法

申　请　人：　联想（北京）有限公司

发明人或设计人：　代华锋、郑轶民



中华人民共和国
国家知识产权局局长　王景川

2004 年 7 月 9 日

权 利 要 求 书

1、一种基于 USB 闪存盘存储介质私有空间的验证方法，其特征在于，至少包括：

步骤 10：验证模块从 USB 闪存盘存储介质的私有空间中读出验证信息；

步骤 20：验证模块根据从 USB 闪存盘中读出的验证信息对用户输入的验证信息进行验证；

步骤 30：判断验证是否成功，如果成功，则开放基于验证信息的操作权限，否则，执行验证失败的处理。

2、根据权利要求 1 所述基于 USB 闪存盘存储介质私有空间的验证方法，其特征在于，在所述步骤 10 之前还包括：

步骤 1：检测 USB 闪存盘是否和验证模块保持连接，如果是则执行步骤 10；

步骤 2：询问用户是否重新验证；如果用户确认重新验证，则提示用户插入 USB 闪存盘，用户确认后执行步骤 1；否则验证失败，进行失败处理。

3、根据权利要求 2 所述基于 USB 闪存盘存储介质私有空间的验证方法，其特征在于，步骤 30 中所述的验证失败的处理为：执行步骤 2。

4、根据权利要求 1 所述基于 USB 闪存盘存储介质私有空间的验证方法，其特征在于，在所述步骤 10 之前还包括：

步骤 1'：验证模块检测 USB 闪存盘是否与其保持连接；

步骤 2'：是，则经过预定时间后执行步骤 1'，否则，锁定系统；

步骤 3'：提示用户插入 USB 闪存盘并输入验证信息；

步骤 4'：验证模块检测 USB 闪存盘是否与其保持连接；

步骤 5'：是则执行步骤 10，否则执行步骤 3'。

5、根据权利要求 4 所述基于 USB 闪存盘存储介质私有空间的验证方法，其特征在于，步骤 30 中所述的验证失败的处理为：如果成功，则解除锁定，执行步骤 1'，否则执行步骤 4'。

6、根据权利要求 1 所述基于 USB 闪存盘存储介质私有空间的验证方法，其特征在于，所述 USB 闪存盘存储介质私有空间中的验证信息在安装验证模块时的设置包括如下步骤：

步骤 A：验证模块将用户输入的验证信息发到 USB 闪存盘存储介质的私有空间；

步骤 B：判断写操作是否成功，如果成功，则开放基于验证信息的操作权限，否则，执行失败的后续操作。

7、根据权利要求 6 所述基于 USB 闪存盘存储介质私有空间的验证方法，其特征在于：所述的验证信息中包含用户的操作系统登录信息。

8、根据权利要求 6 或 7 所述基于 USB 闪存盘存储介质私有空间的验证方法，其特征在于，在所述步骤 A 之前还包括：

步骤 X：验证模块对 USB 闪存盘是否与其正常连接进行检测；如果是，则执行步骤 A；

步骤 Y：询问用户是否重试；如果用户确认重试，则提示用户插入 USB 闪存盘，用户确认后执行步骤 X；否则验证失败，结束设置。

9、根据权利要求 8 所述基于 USB 闪存盘存储介质私有空间的验证方法，其特征在于，步骤 B 中所述的失败的后续操作为：执行步骤 Y。

10、根据权利要求 1 所述基于 USB 闪存盘存储介质私有空间的验证方法，其特征在于：所述 USB 闪存盘的控制芯片接收验证模块发来的读/写指令，判断是否为对私有空间进行读/写操作，如果是则对私有空间进行读/写操作，否则对正常空间进行读/写操作。

说　明　书

基于 USB 闪存盘存储介质私有空间的验证方法

技术领域

本发明涉及一种基于USB闪存盘的验证方法，特别是涉及一种基于USB闪存盘存储介质私有空间的验证方法，属于计算机安全领域。

背景技术

现有的计算机一般不具备加密装置。在现在社会，个人计算机的私密性越来越受到重视，特别注重商业机密和个人资料的安全性。现有的计算机加密功能一般由软件来实现，但是软件被破解的可能性越来越大，计算机上的信息也越来越不安全。目前市场上存在使用硬件加密的方法，主要是使用Smart Card，指纹识别，硬件加密狗，但这些方法存在以下缺点：

1. 缺乏普遍性，涵盖范围窄，比如很多计算机并不支持Smart Card;
2. 机构和电路实现复杂，造成成本偏高；
3. 这种加密硬件功能单一，对用户来说并无太大的优点。

目前也有通过通用串行总线(Universal Serial Bus,简称USB)闪存盘加密的产品，但是加密信息放置于普通空间，普通用户就可以查看、复制及删除，加密的安全性得不到很好保证。

发明内容

本发明的主要目的是提供一种基于USB闪存盘存储介质私有空间的验证方法，使用目前常用的USB闪存盘，通过和验证软件结合，利用一般用户看不到、不能复制也删除不了的USB闪存盘私有空间存储加密信息和加密文件，实现安全可靠，方便易用的计算机加密及验证。

本发明的目的是通过以下技术方案实现的：

一种基于 USB 闪存盘存储介质私有空间的验证方法，至少包括：

步骤 10：验证模块从 USB 闪存盘存储介质的私有空间中读出验证信息；

步骤 20：验证模块根据从 USB 闪存盘中读出的验证信息对用户输入的验证信息进行验证；

步骤 30：判断验证是否成功，如果成功，则开放基于验证信息的操作权限，否则，执行验证失败的处理。

在所述步骤 10 之前还包括：

步骤 1：检测 USB 闪存盘是否和验证模块保持连接，如果是则执行步骤 10；

步骤 2：询问用户是否重新验证；如果用户确认重新验证，则提示用户插入 USB 闪存盘，用户确认后执行步骤 1；否则验证失败，进行失败处理。

步骤 30 中所述的验证失败的处理为：执行步骤 2。

或者：在所述步骤 10 之前还包括：

步骤 1'：验证模块检测 USB 闪存盘是否与其保持连接；

步骤 2'：是，则经过预定时间后执行步骤 1'，否则，锁定系统；

步骤 3'：提示用户插入 USB 闪存盘并输入验证信息；

步骤 4'：验证模块检测 USB 闪存盘是否与其保持连接；

步骤 5'：是则执行步骤 10，否则执行步骤 3'。

步骤 30 中所述的验证失败的处理为：如果成功，则解除锁定，执行步骤 1'，否则执行步骤 4'。

所述 USB 闪存盘存储介质私有空间中的验证信息在安装验证模块时的设置包括如下步骤：

步骤 A：验证模块将用户输入的验证信息发送到 USB 闪存盘存储介质的私有空间；

步骤 B：判断写操作是否成功，如果成功，则开放基于验证信息的操作权限，否则，执行失败的后续操作。

所述的验证信息中包含用户的操作系统登录信息。

上述步骤 A 之前还包括：

步骤 X：验证模块对 USB 闪存盘是否与其正常连接进行检测，如果是，则执行步骤 A；

步骤 Y：询问用户是否重试；如果用户确认重试，则提示用户插入 USB 闪存盘，用户确认后执行步骤 X；否则验证失败，结束设置。

步骤 B 中所述的失败的后续操作为：执行步骤 Y。

上述 USB 闪存盘的控制芯片接收验证模块发来的读/写指令，判断是否为对私有空间进行读/写操作，如果是则对私有空间进行读/写操作，否则对正常空间进行读/写操作。

综上所述，本发明实现一个使用目前常用的USB闪存盘存储介质私有空间进行验证的模块，USB闪存盘的控制芯片接收验证模块发来的读/写指令，判断是否为对私有空间进行读/写操作，如果是则对私有空间进行读/写操作，否则对正常空间进行读/写操作；这样就利用了一般用户看不到、不能复制也删除不了的USB闪存盘私有空间存储各种验证信息，也可以用USB闪存盘正常空间存储一般数据，实现安全可靠，方便易用的加密及验证机制。

附图说明

图1为本发明安全软件与USB闪存盘结合的安全认证机制的结构图；

图2为本发明使用的USB闪存盘读写函数关系图；

图3为本发明安全软件安装时写入USB闪存盘密码流程图；

图4为本发明在操作系统启动时进行验证的流程图；

图5为本发明对于USB闪存盘的监控以及USB闪存盘拔除后的验证流程图；

图6为使用本发明方法进行文件加密的流程图；

图7为使用本发明方法进行文件解密的流程图。

具体实施方式

以下，结合具体实施例并参照附图，对本发明做进一步的详细说明。

如图1所示，本发明方法在操作系统中安装有安全软件，通过USB接口与USB闪存盘进行信息交换。

如图2所示，在计算机和USB闪存盘之间利用函数进行信息交换；计算机将文件信息读出/写入USB闪存盘的正常空间，调用的函数是ReadUdisk（参数1）/WriteUdisk（参数1）；将文件信息读出/写入USB闪存盘的私有空间，调用的函数是ReadPrivateBYTES（参数1）/ WritePrivateBYTES（参数1）；上述两组函数最终都转化为读/写函数Read（参数1，参数2）/Write（参数1，参数2）进行底层读写操作，其中参数1是需要读写的内容，参数2是对于正常/私有空间的判断。USB闪存盘的控制芯片对读/写函数的参数2进行判断，如果参数2是“私有”，那么控制芯片将从闪存芯片中的私有空间开始读取，如果参数2不是“私有”，那么控制芯片将从正常的空间开始读取。

私有空间（PrivateBYTES）和正常空间(NormalBYTES)的区别：

私有空间也可以称作保留区域，产品出厂设定，可以通过专门工具写入存储内容，用户无法改变其属性大小和内容，也看不到，无法格式化。

正常空间：用户可以正常使用的存储区域，拥有完全控制的权利。

如图3所示，安全软件安装时，需要将用户设定的密码和其他认证信息写入USB闪存盘，包括如下步骤：

步骤101：安装安全软件；

步骤102：初始化安全软件，收集操作系统登录信息，例如用户名及其登录密码；

步骤103：对USB闪存盘是否正常连接进行检测；

步骤104：根据步骤103的检测结果判断USB闪存盘是否正常连接；如果

是执行步骤107；

步骤105：询问用户是否结束安装；如果用户确认结束，则退出安全软件，安装流程结束，软件安装没有成功完成；

步骤106：提示用户插入USB闪存盘，用户确认插入后执行步骤103；

步骤107：用户输入USB闪存盘密码；

步骤108：将操作系统登录信息和USB闪存盘密码形成加密文件；

步骤109：将密码写入USB闪存盘的私有空间或正常空间中；

步骤110：判断写入是否成功，如果是则执行步骤111，否则执行步骤105；

步骤111：安全软件安装成功；重新启动操作系统。

如图4所示，每次操作系统启动时，安全软件在用户登录前先对用户进行安全认证，若认证通过则根据USB闪存盘中存储的操作系统登录信息自动登录，否则关闭操作系统，具体步骤如下：

步骤201：启动操作系统；

步骤202：对USB闪存盘是否正常连接进行检测；

步骤203：根据步骤202的检测结果判断USB闪存盘是否正常连接；如果是执行步骤206，否则执行步骤204；

步骤204：询问用户是否重试；如果用户确认是，则执行步骤205，否则关闭操作系统；

步骤205：提示用户插入USB闪存盘，用户确认插入后执行步骤202；

步骤206：用户输入USB闪存盘密码；

步骤207：读USB闪存盘的验证信息；

步骤208：根据验证信息对用户输入的密码进行验证；

步骤209：判断验证是否成功，如果是则执行步骤210，否则执行步骤204；

步骤210：根据USB闪存盘中存储的操作系统登录信息自动登录操作系统。

如图5所示，系统正常运行时，安全软件对USB闪存盘状态定时进行检测；

用户暂时不用系统时，可不必关闭系统，而只需将USB闪存盘拔下；安全软件检测到USB闪存盘不存在，则自动将系统锁定，只有插入USB闪存盘并通过相应的安全认证，安全软件才将系统解除锁定，重新进入正常操作状态；步骤如下：

步骤301：用户正常操作时，安全软件对USB闪存盘定时检测；

步骤302：根据步骤301的检测结果判断USB闪存盘是否正常连接；如果是执行步骤301，否则执行步骤303；

步骤303：系统锁定；

步骤304：提示用户插入USB闪存盘；

步骤305：用户插入USB闪存盘后安全软件对USB闪存盘是否正常连接进行检测；

步骤306：根据步骤305的检测结果判断USB闪存盘是否正常连接；如果是执行步骤307，否则执行步骤304；

步骤307：用户输入USB闪存盘密码；

步骤308：读USB闪存盘的验证信息；

步骤309：根据验证信息对用户输入的密码进行验证；

步骤310：判断验证是否成功，如果是则执行步骤311，否则执行步骤304；

步骤311：解除系统锁定，执行步骤301。

如图6所示，本发明方法还可用于文件的加/解密，用安全软件和USB闪存盘加密文件包括以下步骤：

步骤501：确定需要加密的文件；

步骤502：对USB闪存盘是否正常连接进行检测；

步骤503：根据步骤502的检测结果判断USB闪存盘是否正常连接；如果是执行步骤506，否则执行步骤504；

步骤504：询问用户是否重试；如果用户确认是，则执行步骤505，否则退出加密流程，该文件没有被加密；

步骤505：提示用户插入USB闪存盘，用户确认插入后执行步骤502；

步骤506：用户输入加密密码；

步骤507：将验证信息写入USB闪存盘的私有空间；

步骤508：判断写入是否成功，如果是则执行步骤509，否则执行步骤504；

步骤509：将正常文件转换为加密文件。

如图7所示，对用安全软件和USB闪存盘加密的文件进行解密包括以下步骤：

步骤401：确定需要解密的文件；

步骤402：对USB闪存盘是否正常连接进行检测；

步骤403：根据步骤402的检测结果判断USB闪存盘是否正常连接；如果是执行步骤406，否则执行步骤404；

步骤404：询问用户是否重试；如果用户确认是，则执行步骤405，否则退出解密流程，该文件仍旧处于加密状态；

步骤405：提示用户插入USB闪存盘，用户确认插入后执行步骤402；

步骤406：用户输入解密密码；

步骤407：读USB闪存盘的验证信息；

步骤408：根据验证信息对用户输入的密码进行验证；

步骤409：判断验证是否成功，如果是则执行步骤410，否则执行步骤404；

步骤410：将加密文件还原成正常文件。

本实施例USB闪存盘存储介质的私有空间中存储的各种验证信息都可以在系统正常运行时通过安全软件更改，更改时需保证USB闪存盘和系统正常连接，并且输入正确的具有修改权限的密码。

最后所应说明的是，以上实施例仅用以说明本发明的技术方案而非限制，尽管参照较佳实施例对本发明进行了详细说明，本领域的普通技术人员应当理解，可以对本发明的技术方案进行修改或者等同替换，而不脱离本发明技术方案的精神和范围，其均应涵盖在本发明的权利要求范围当中。

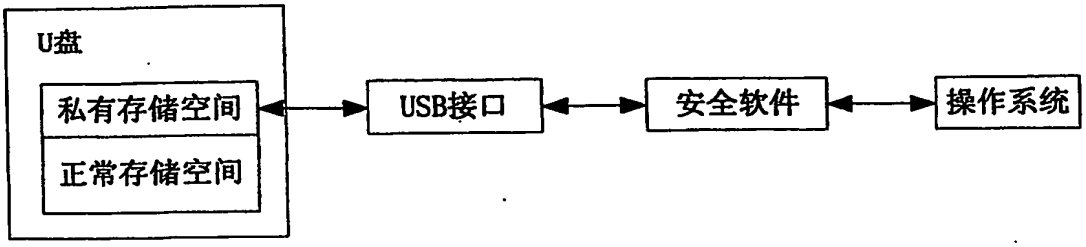

U盘
私有存储空间
正常存储空间
USB接口
安全软件
操作系统

图 1

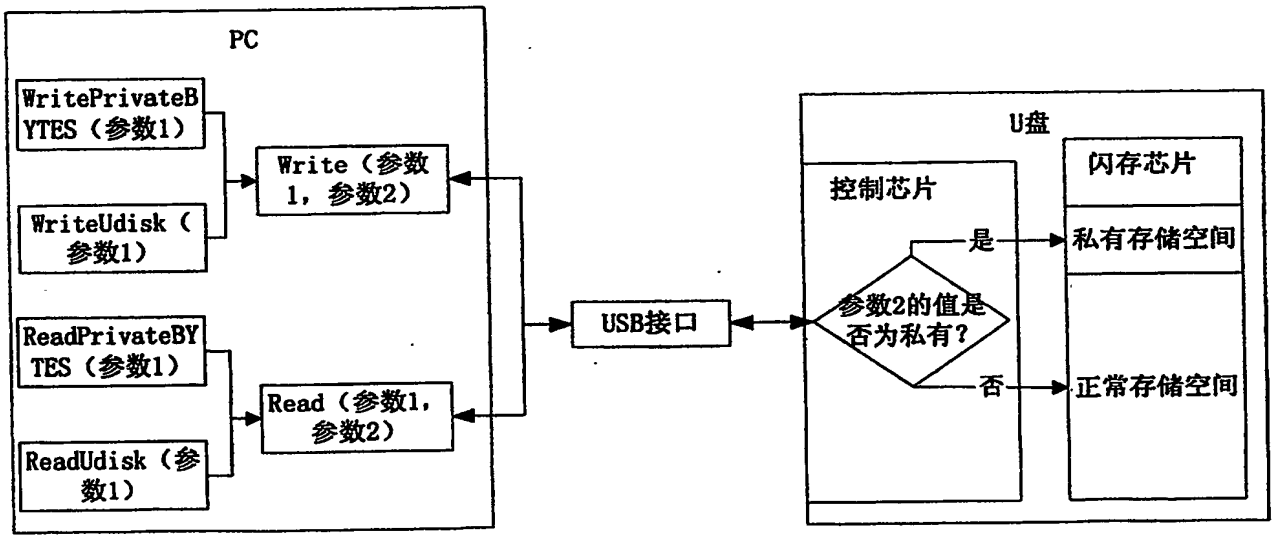

PC
WritePrivateBYTES（参数1）
WriteUdisk（参数1）
Write（参数1，参数2）
ReadPrivateBYTES（参数1）
ReadUdisk（参数1）
Read（参数1，参数2）
USB接口
U盘
控制芯片
闪存芯片
参数2的值是否为私有？
是
否
私有存储空间
正常存储空间

图 2

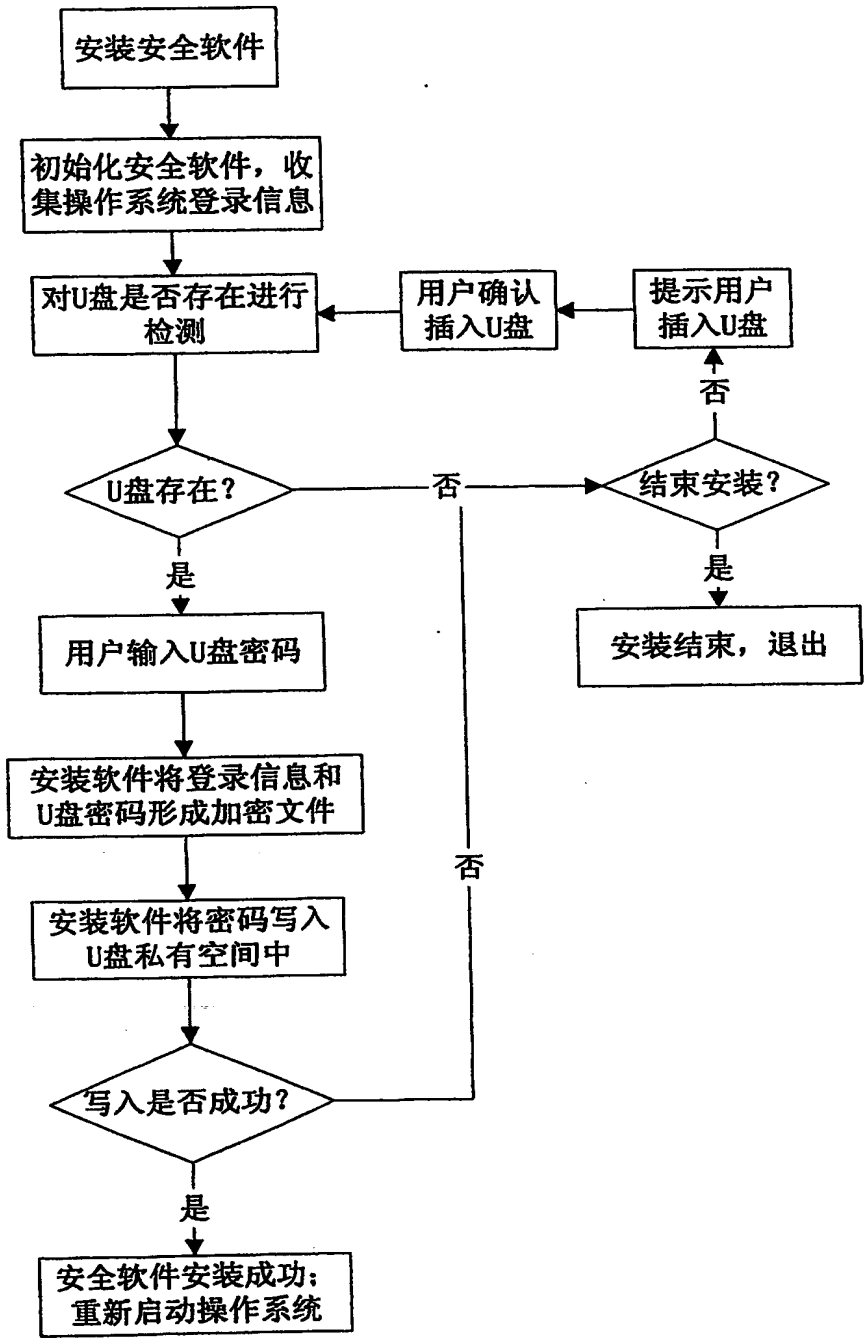

安装安全软件
初始化安全软件，收集操作系统登录信息
对U盘是否存在进行检测
用户确认插入U盘
提示用户插入U盘
否
U盘存在？
否
结束安装？
是
是
用户输入U盘密码
安装结束，退出
安装软件将登录信息和U盘密码形成加密文件
安装软件将密码写入U盘私有空间中
否
写入是否成功？
是
安全软件安装成功；重新启动操作系统

图 3

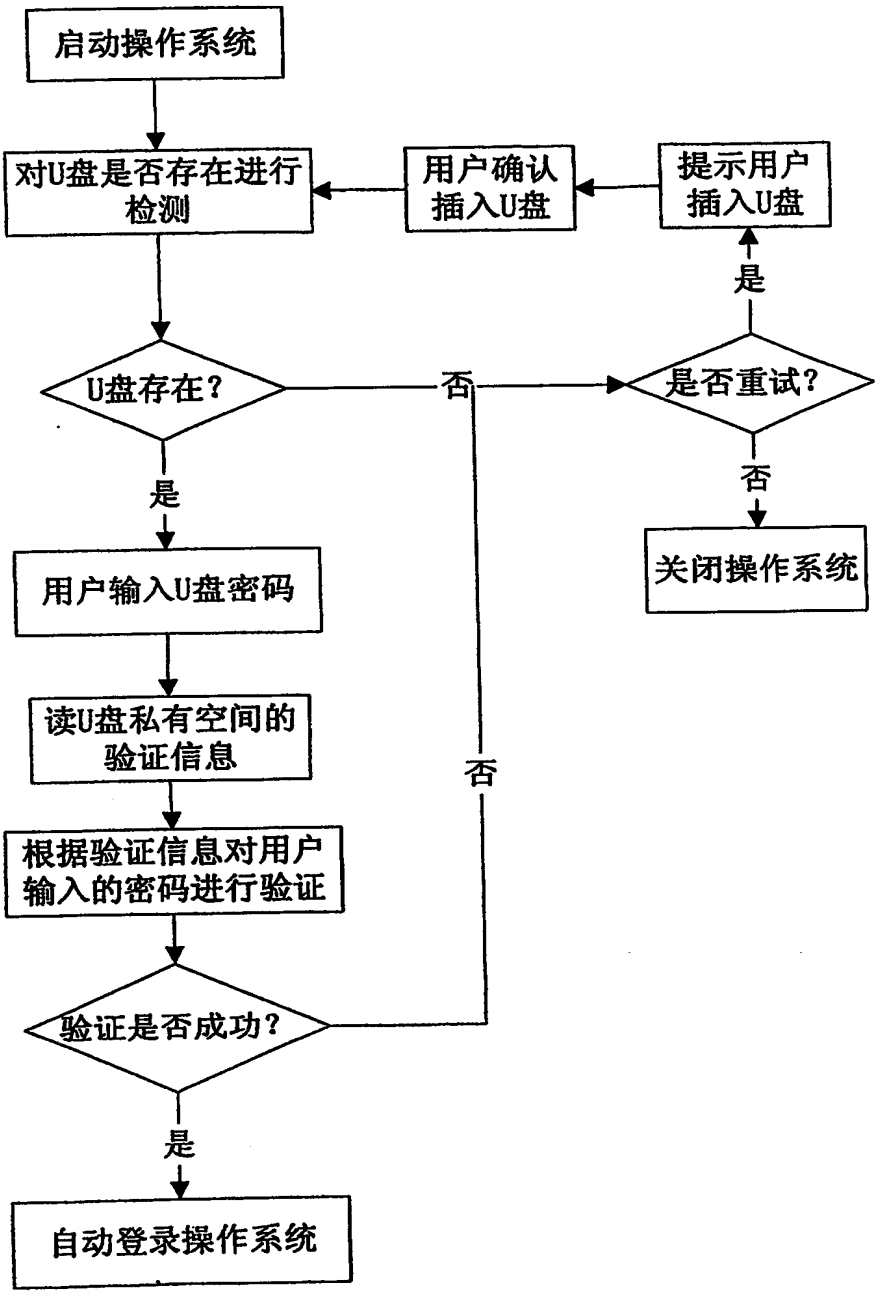

启动操作系统
对U盘是否存在进行检测
用户确认插入U盘
提示用户插入U盘
是
U盘存在？
否
是否重试？
否
关闭操作系统
是
用户输入U盘密码
读U盘私有空间的验证信息
根据验证信息对用户输入的密码进行验证
否
验证是否成功？
是
自动登录操作系统

图 4

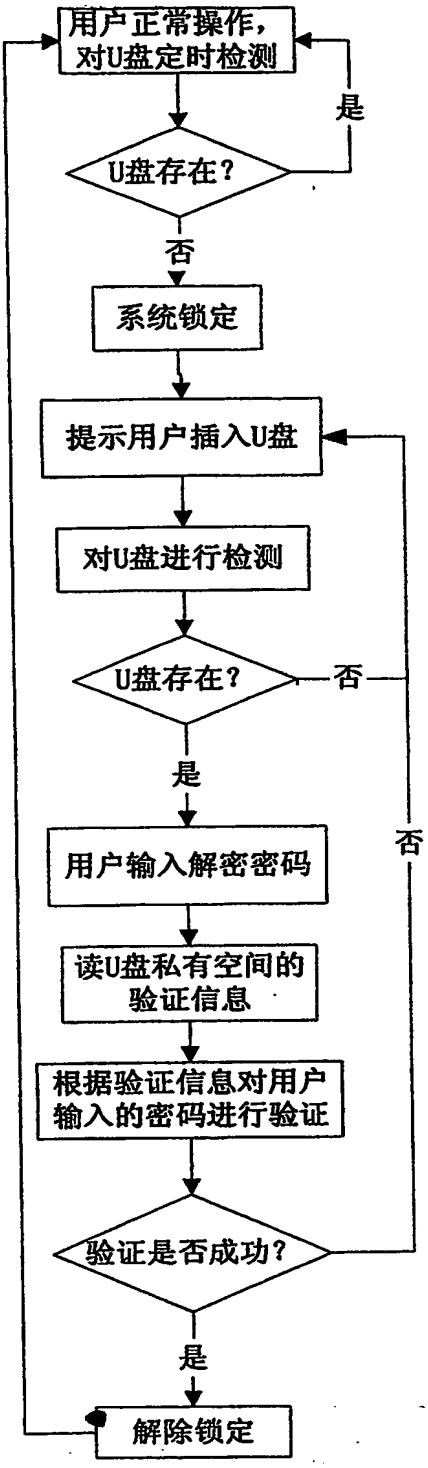

用户正常操作，对U盘定时检测
是
U盘存在？
否
系统锁定
提示用户插入U盘
对U盘进行检测
U盘存在？
否
是
否
用户输入解密密码
读U盘私有空间的验证信息
根据验证信息对用户输入的密码进行验证
验证是否成功？
是
解除锁定

图 5

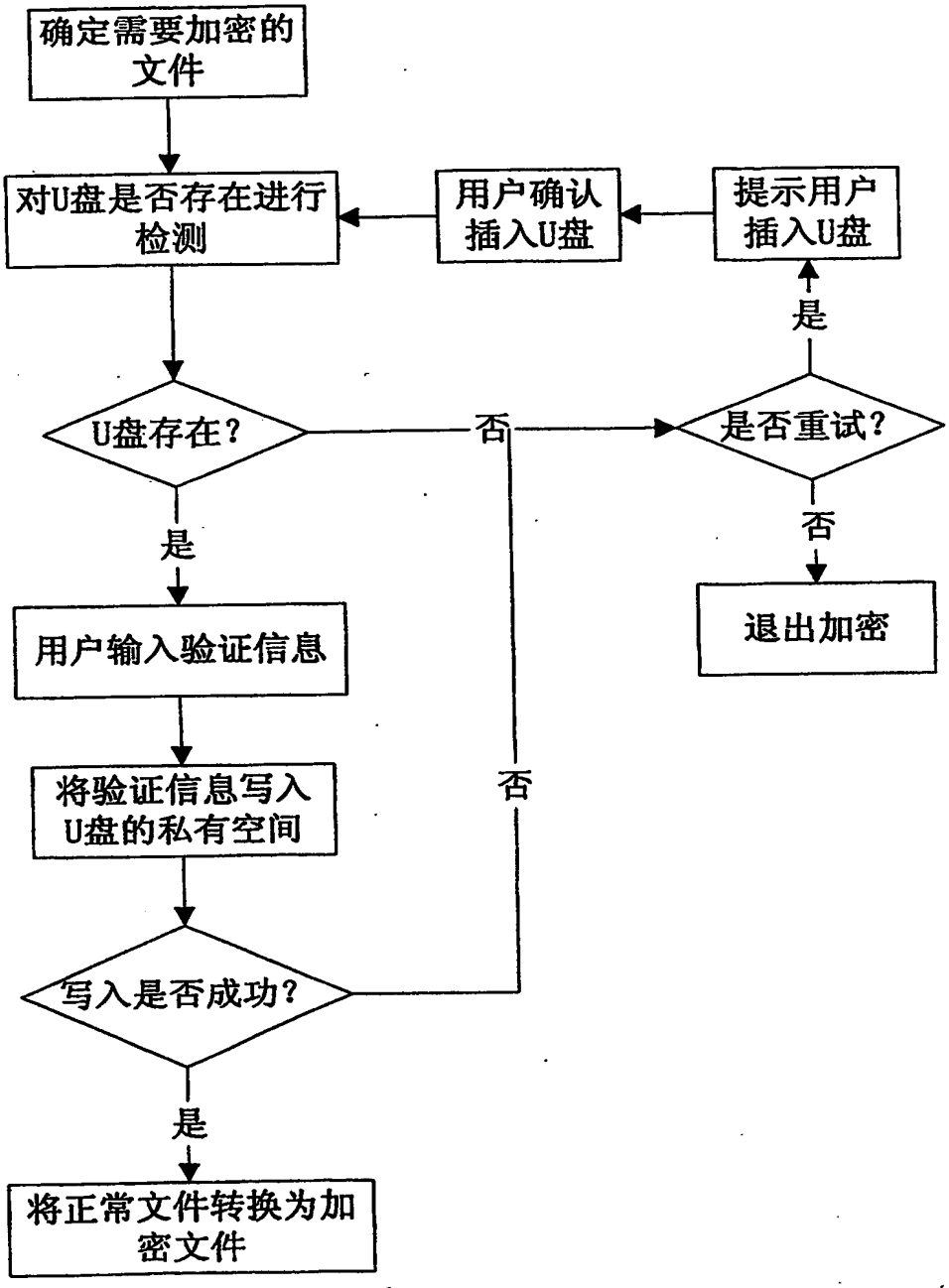

确定需要加密的文件
对U盘是否存在进行检测
用户确认插入U盘
提示用户插入U盘
U盘存在？
否
是否重试？
是
否
退出加密
是
用户输入验证信息
将验证信息写入U盘的私有空间
写入是否成功？
否
是
将正常文件转换为加密文件

图 6

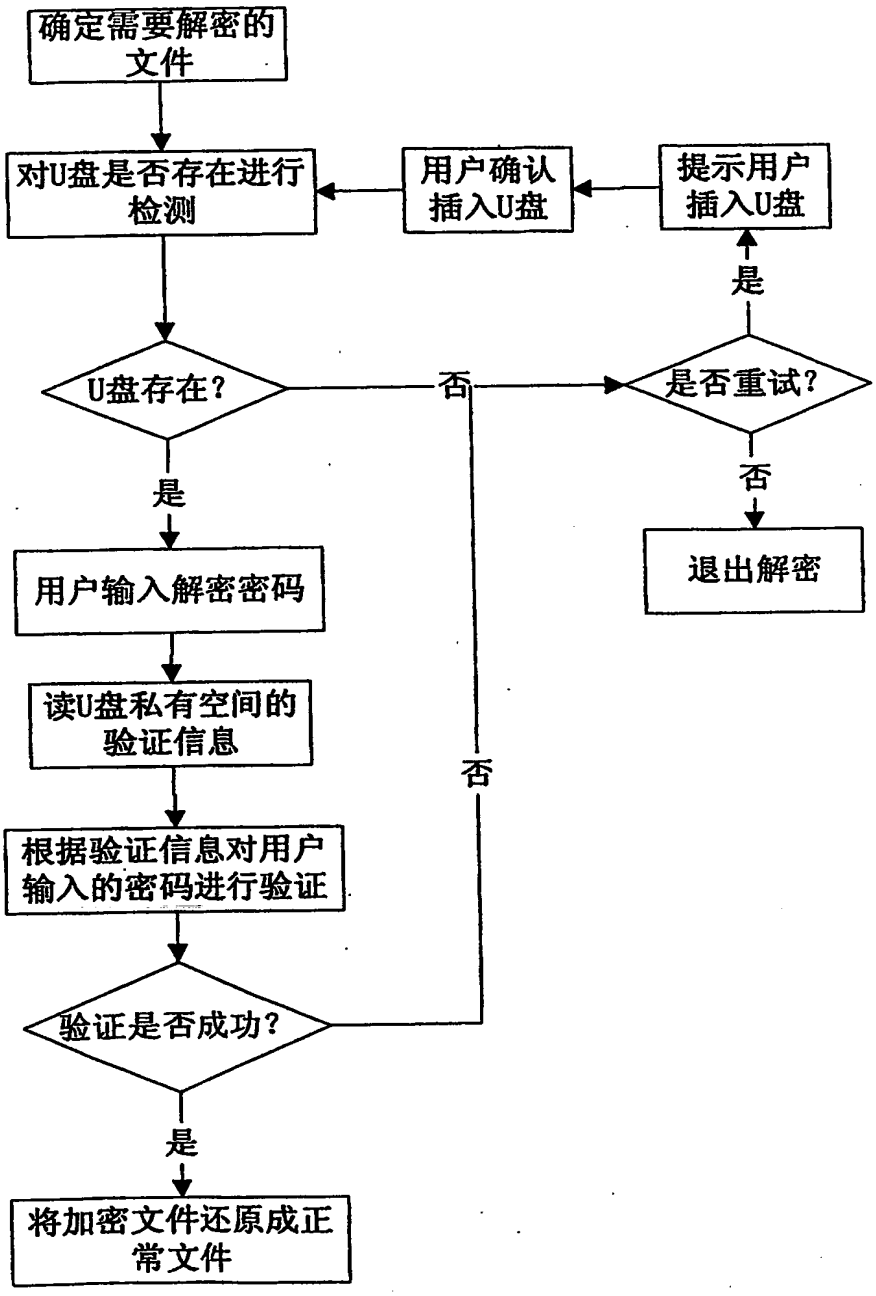

确定需要解密的文件
对U盘是否存在进行检测
用户确认插入U盘
提示用户插入U盘
是
U盘存在？
否
是否重试？
否
是
退出解密
用户输入解密密码
读U盘私有空间的验证信息
根据验证信息对用户输入的密码进行验证
否
验证是否成功？
是
将加密文件还原成正常文件

图 7